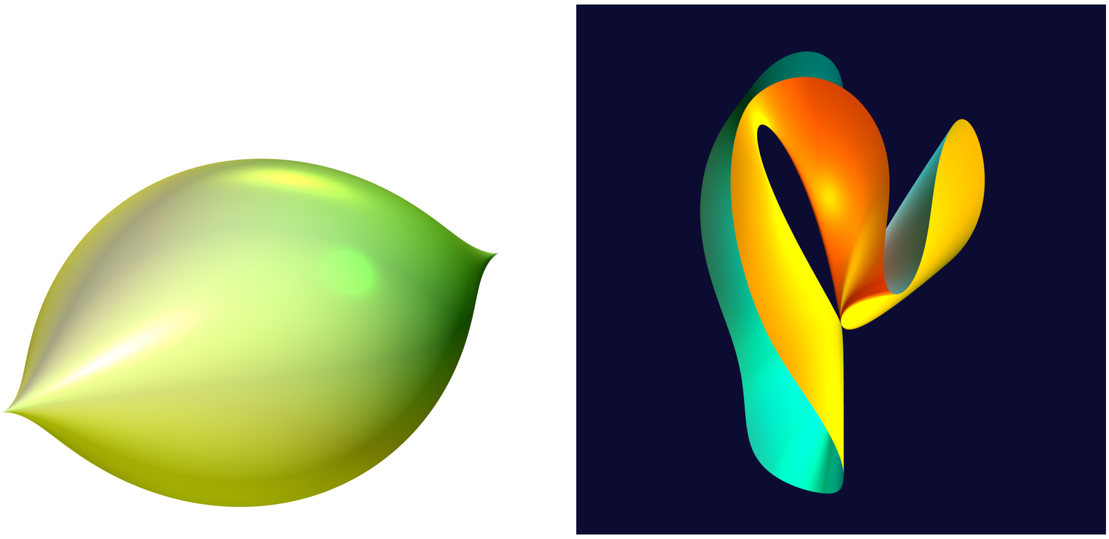
Algebra, Number Theory, Algebraic Geometry

Algebra is concerned with solving polynomial equations, like $X^2 - 2 = 0$ oder $X^5 - 4X + 2 = 0$. While the solutions $X = \pm\sqrt{2}$ of the first equation can be obtained by taking roots, this is not possible for the second equation. This fact can be proven by using the ingenious ideas of E. Galois, who was killed in 1832 at the age of 21 in a duel. The theory of Galois is explained in the lecture “Algebra” which one usually takes in a Bachelor of Science in Mathematics. There, one also learns why squaring the circle and dividing an angle in three equal parts is impossible with ruler and compas.

Now we consider all polynomial equations $X^n + a_{n-1}X^{n-1} + \ldots + a_1X^1 + a_0 = 0$, where $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ are rational numbers. We denote by $\overline{\mathbb{Q}}$ the set of all numbers which are solutions of one of these equations. Then $\overline{\mathbb{Q}}$ forms a *field*, i.e. the sum, difference, product, and quotient of two numbers from $\overline{\mathbb{Q}}$ again belongs to $\overline{\mathbb{Q}}$. (For example, $\sqrt{2} + \sqrt{3}$ is solution of the equation $X^4 - 10X^2 + 1 = (X^2 - 5)^2 - 24 = 0$.) One of the central problems of current research in Algebra and *Number Theory* is to understand the field $\overline{\mathbb{Q}}$ better. We will come back to this below.

After having investigated solutions of polynomial equations in one variable X above, it is natural to also study solution sets of polynomial equations (or systems of polynomial equations) in several variables, like $X^2 + Y^2 - 1 = 0$ or $Y^2 - X^3 - 17 = 0$. These solution sets have a geometric structure: for example, the circle is the solution set of $X^2 + Y^2 - 1 = 0$, and $Y^2 - X^3 - 17 = 0$ is drawn in Figure 2 on the next page.



(a) $X^2 + Z^2 + Y^3(Y-1)^3 = 0$
“Citric (Zitrus)”

(b) $(X^2 - Y^3)^2 - (X + Y^2)Z^3 = 0$
“Seahorse (Seepferdchen)”

©Herwig Hauser, Source https://www.imaginary.org/gallery/herwig-hauser-classic

Figure 1: solutions of the respective equation with values in the real numbers

Moreover, in Figure 1 solution sets of one equation in three variables X, Y, Z are shown. All such solution sets also have a rich algebraic structure that originates from considering polynomial equations. The area of mathematics which investigates such solution sets is called *Algebraic Geometry*. In this area, also aspects of Topology and Analysis play an important role. Algebraic Geometry and Algebraic Number Theory have long been important areas of international mathematical research.

A very interesting collection of solution sets is obtained by equations of the form $Y^2 - X^3 - aX - b = 0$ for $a, b \in \mathbb{Q}$. The points in such a solution set can be "added" by the following rule. If P, Q are two points in the solution set, one considers the line g passing through P and Q, like in Figure 2. (In case $P = Q$, one takes g as the tangent in P to the solution set.) The line g intersects the solution set in another point R (which is equal to P or Q if $P \neq Q$ and g is the tangent in P or Q). Reflecting R at the X-achsis, one obtains the point S that also belongs to the solution set. The "addition law" now defines S as the "sum" of P and Q. We write $P \oplus Q = S$. Obviously $P \oplus Q = Q \oplus P$.

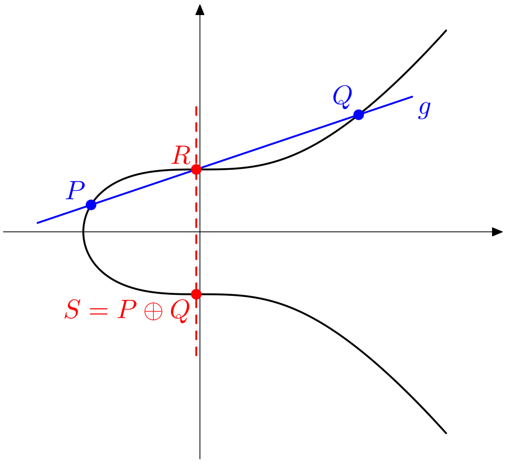


Figure 2: Addition law on the curve $Y^2 - X^3 - 17 = 0$

Furthermore, $(P \oplus Q) \oplus T = P \oplus (Q \oplus T)$, if T is another point in the solution set, but this is by no means obvious. If the coordinates of P and Q lie in the rational numbers $\mathbb{Q}$, then this is also true for $P \oplus Q$. In this way one sees that the equation $Y^2 - X^3 - 17 = 0$ has infinitely many solutions with rational coefficients (for example, $(-2, 3)\,, (2, 5)\,, (\frac{137}{64}, -\frac{2651}{512})\,, \ldots$). Concerning the "degree" of this infinity, there is a famous conjecture of B. Birch and P. Swinnerton-Dyer, which is a Millenium Prize Problem whose solution is worth 1 million US-dollars in prize money.

Another famous conjecture, which was unsolved for more than 350 years, is the conjecture of the number theorist P. de Fermat which says that the equation $X^n + Y^n - Z^n = 0$ has no solutions in the rational numbers $\mathbb{Q}$ with $X \cdot Y \cdot Z \neq 0$ if n is an integer greater than 2. This conjecture could be proven in 1994 in a spectacular way with the help of Algebraic Geometry. Also to the understanding of the field $\overline{\mathbb{Q}}$, Algebraic Geometry makes valuable contributions in many ways by considering systems of polynomial equations with coefficients in $\mathbb{Q}$.

Yet another Millenium Prize Problem worth 1 million US-dollars is the Riemann conjecture. It is concerned with counting prime numbers which are $\leq N$ for a given real number N. One knows that there are approximately $\int_2^N \frac{dt}{\ln t}$ many primes. The question now is to specify and prove the optimal error estimate for this easily calculable approximation. For this purpose, Zeta and L-functions play a major role. These are also used in the conjecture of Birch and Swinnerton-Dyer and in other areas of number theory.

At the University of Münster, Number Theory and Algebraic Geometry are an important research focus with a long tradition. At present, the research groups of four professors with around fifteen members work in this this area. This focus also plays an important role in the Bachelor's and Master's degree programs.